## AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1 – 2. (Cancelled)

3. (New) A key management system comprising:

a unit which defines a tree structure assigning plural information receivers to leaves;

a unit which divides the tree structure into macrolayers of a predetermined number to define plural subtrees;

a unit which independently defines differential subsets of the information receivers for each of the subtrees, the subset being defined by an ancestor node and a descendant node existing in the subtree, the information receivers being assigned to the leaves of the subtree which exist at a layer identical to or below the ancestor node and does not exist at a layer identical to or below the descendant node or assigned to the leaves of the tree structure which exist at a layer below the leaves of the subtree;

a unit which assigns one encryption/decryption key to each of the differential subset; and

a unit which assigns, to each of the plural information receivers, the encryption/decryption key assigned to all the differential subsets to which the information receiver belong.

4. (New) The key management system according to claim 1, further comprising a key information generating unit which generates key information decryptable only by specific information receivers in the plural information receivers assigned to the leaves of the tree structure.

5. (New) The key management system according to claim 1, further comprising a unit which assigns, to specific information receivers in the plural information receivers, confidential information which enables to derive the encryption/decryption key assigned to all the differential subsets including the information receivers.

6. (New) The key management system according to claim 1, further comprising:

a key information generating unit which generates key information decryptable only by specific information receivers in the plural information receivers assigned to the leaves of the tree structure;

a unit which assigns, to the specific information receivers, confidential information which enables to derive the encryption/decryption key assigned to all the differential subsets including the information receivers; and

a unit which derives the encryption/decryption key assigned to all the differential subsets including the specific information receivers by using the key information and the confidential information.

7. (New) A key management method comprising:

a process which defines a tree structure assigning plural information receivers to leaves ;

a process which divides the tree structure into macrolayers of a predetermined number to define plural subtrees;

a process which independently defines differential subsets of the information receivers for each of the subtrees, the subset being defined by an ancestor node and a descendant node existing in the subtree, the information receivers being assigned to the leaves of the subtree which exist at a layer identical to or below the ancestor node and does not exist at a layer identical to or below the descendant node or assigned to the leaves of the tree structure which exist at a layer below the leaves of the subtree;

a process which assigns one encryption/decryption key to each of the differential subset; and

a process which assigns, to each of the plural information receivers, the encryption/decryption key assigned to all the differential subsets to which the information receiver belong.

8. (New) A computer product program in a computer-readable medium executed by a key management system comprising a computer, the computer product program making the computer function as:

a unit which divides the tree structure into macrolayers of a predetermined number to define plural subtrees;

a unit which independently defines differential subsets of the information receivers for each of the subtrees, the subset being defined by an ancestor node and a descendant node existing in the subtree, the information receivers being assigned to the leaves of the subtree which exist at a layer identical to or below the ancestor node and does not exist at a layer identical to or below the descendant node or assigned to the leaves of the tree structure which exist at a layer below the leaves of the subtree;

a unit which assigns one encryption/decryption key to each of the differential subset; and

a unit which assigns, to each of the plural information receivers, the encryption/decryption key assigned to all the differential subsets to which the information receiver belong.

9. (New) A recording medium which records the key information generated by the key management system according to claim 2.